FEDERAL PKI POLICY AUTHORITY

November 6, 2012 MEETING MINUTES

GSA NOMA
One Constitution Square
Conference Room 401
1275 1st Street, NE,
Washington, DC 20417
10:00 a.m. – 11:45 a.m. EST

10:00	**Welcome, Opening Remarks & Introductions**	**Deb Gallagher, Chair**
10:05	**Discussion/Vote: October 2012 FPKIPA Minutes**	**Matt King**
10:10	**FPKI Certificate Policy Working Group (CPWG) Report** **1. Discussion/Vote: PIV Content Signing Policy Change Proposal (Common CP)** **2. Mapping Updates** **3. Other Updates**	**Charles Froehlich**
10:40	**SHA-1 Transition Status**	**SHA-1 Affiliates**
10:45	**VA Status Update**	**John Hancock**
11:00	**FPKIPA Chair Update**	**Deb Gallagher**
11:30	**Other Agenda Items** o *If you cannot attend, please designate a proxy* o *Next FPKIPA meeting, December 11, 2012*	**Deb Gallagher**
11:45	**Adjourn Meeting**	**Deb Gallagher**

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Bures, Iva	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	P
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	T
Department of Justice (DOJ)	Morrison, Scott	A
Department of State (State)	Steve Gregory	A
Department of Treasury (Treasury)	Wood, Dan	A
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	A
United States Postal Service (USPS)	Stepongzi, Mark	T
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	T
Veterans Administration (VA)	Jurasas, Eric	A

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
DoD	Baldridge, Tim	T
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
FPKIMA (Contractor, Protiviti)	Cimmino, Giuseppe	T
IdenTrust	Cox, Jerry	T
DoD (Contractor)	Frank, Larry	T
DoS (Contractor, ManTech)	Froehlich, Charles	P
Treasury	Johnson, Todd	T
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIPA (Contractor, Protiviti)	Louden, Chris	P
Veterans Administration (VA)	Muir, Tom	P
DHA (Contractor)	Shomo, Larry	T
FPKIPA (Contractor, Protiviti)	Silver, Dave	T

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at GSA NOMA One Constitution Square, Conference Room 401, 1275 1st Street, NE, Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 10:03 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on October 16, 2012 FPKIPA Minutes, Matt King

There was a vote to approve the October 16, 2012 FPKIPA minutes. HHS motioned to approve; NRC seconded. The motion was approved unanimously.

Approval Vote for October 16, 2012 FPKIPA Minutes			
Voting members	**Vote (HHS Motion; NRC Seconded)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ) – Proxy to GSA	√		
Department of State (State) – Proxy to GSA	√		
Department of the Treasury (Treasury)			Absent
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)			Absent
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)			Absent

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

Mr. Charles Froehlich presented the CPWG Report.

a. Discussion/Vote: PIV Content Signing Policy Change Proposal

This change proposal has been under discussion for several months. The stated purpose was that FIPS 201-2 requires the devicesHardware policy OID plus the PIV Content Signing EKU for certificates issued to CMSs. NIST will reference a PIV Common Content Signing Policy OID in FIPS 201 if it is included in the FCPCA CP. The PIV Common Content Signing Policy needs to be defined in the Common Policy in time for FIPS 201 to reference it. Adding this policy OID might also provide an opportunity to strengthen Common Policy requirements and provide an opportunity to define narrower requirements for certificates issued to CMSs.

The CPWG has been unable to reach consensus. It has been suggested that the question of the policy OID be separated from CMS requirements. However, others believe that the two are irrevocably linked. It has also been argued that the FCPCA CP should specify requirements for the CMS, although others believe that the requirements should be applied only to that element doing the actual content signing, and that CMS specific controls if needed should be outlined in either the FIPS 201 or its subordinate Special Publications.

A lengthy discussion was held about the change proposal with the following highlights:

- These requirements only apply if you assert the Content Signing OID.
- Securing the CMS is a critical component of the PKI but there were differing opinions on whether those requirements should appear in the Common Policy or were already covered by FIPS 201.
- Content signing in other areas must also be considered (e.g., mobile devices), but it may not be beneficial to use the same OID to sign identity content as mobile code signing.
- When a relying party decides to trust, they only know whether the PKI meets the policy – so it’s the only thing the FPKI can use to assert that trust.
- Noted that two-person physical control is not practical and not the way CMSs are operated.

After the discussion, it was decided that the change proposal will be sent back to the CPWG for modification to the language regarding CMS requirements.

b. Mapping Updates

DoD is making some final changes to their CP to accommodate CPWG inputs and will address these changes at the next CPWG meeting. The ExoStar mapping has been completed except for some recommended changes. The mapping of USPS will be fully underway at the next CPWG meeting.

c. Other Updates

CertiPath has raised a proposal to develop an international standard, based on the PIV-I requirements in the FBCA CP, to issue PIV-I equivalent cards to non-U.S. persons outside the U.S. by non-U.S. providers that may or may not be used for logical or physical access to U.S. systems or facilities. This is an opinion paper, not a FBCA CP change proposal, and the issue for consideration is whether to forward to the ICAMSC/ISIMC for further review and action.

a) Some believe that this effort is out-of-scope for the CPWG/FPKIPA.
b) The main effort is to eliminate reference to the I-9 list, which is only applicable within the U.S.
c) DoS has only limited authorizations relative to ID document acceptability, and each country has its own unique requirements and prohibitions.
d) There is also the question of relying party acceptance of individual certificates and/or certificates issued by given providers and/or countries - a potential solution being to exclude sub-trees.

It was agreed that Ms. Gallagher will present this paper to the ICAMSC on December 5, 2012.

PIVI IDProofing
nonUS_1NOV12_CPW

The CPWG also addressed a question raised through NIST relating to FIPS 201—should the printed name on a PIV card match the DN?. The CPWG determined that this was unnecessary, and potentially counter-productive given the potential variations in DNs between agencies and relative to a human recognizable name.

SHA-1 Transition Status, SHA-1 Affiliates

No updates were provided.

VA Status Update, John Hancock

Mr. Tom Muir of VA's Office of Security Preparedness presented a report on progress toward addressing issues identified in the September 2011 Office of the Inspector General (OIG) report. Highlights include:

- VA had not done an A&A of some of the facilities. VA has now completed an assessment and accreditation of all 204 sites. All have achieved IATO or ATO status. All have SOPs and staff trained and certified.
- VA now has Separation of Duties.
- When VA finds people who share cards, they now revoke the cards and retrain the staff.
- There was an issue with background investigations. Now VA requires a validated NACI initiation (validate with FIPs).

- VA is working on a process to determine if someone becomes untrustworthy (since NACI’s are good for life, there is no way to tell if people are still in good standing).
- VA started using PIV Cards for physical access and is now using PIV Cards to do initial logon to LACS in the VA central office.
- VA is upgrading PACS readers to be FIPS 201 compliant.

Ms. Gallagher requested that VA contact her before going forward with PACS because there are some physical access initiatives that are part of the President’s management council of which VA may need to be aware. Ms. Gallagher thanked Mr. Muir for the update.

ACTION ITEMS: None

FPKIPA Chair Update, Deb Gallagher

Ms. Gallagher presented the FPKIPA Chair Report. Upcoming meetings and events include:

Meeting	Date
Strong Logical Access Tiger Team (SLATT)	**Wednesdays 10:00 – 11:00am**
ISIMSC	**November 14, 2012**
CPWG	**November 20, 2012**
IAB	**December 5, 2012**
ICAMSC	**December 5, 2012**
ICAM Day	**November 27, 2012**
Mobile Tiger Team	**November 15, 2012**

Ms. Gallagher provided updates on Working Groups and Tiger Teams and mentioned that FCIX is moving forward at USPS. USPS will model this effort after the FPKI, and GSA will be the Policy Authority with USPS as the Operational Authority and the stakeholders as members. A pilot is expected in the first few months of 2013.

FPKIPA Chair
Report_6NOV12.pptx

The next FPKIPA meeting is December 11, 2012. The meeting will be at USPS.

FPKIMA Network Updates, Giuseppe Cimmino

Mr. Giuseppe Cimmino presented a brief report on recent FPKIMA network updates resulting in new IP Addresses for the FPKIMA.

Nov2012 PA Meeting
FPKIMA Gen 2 Slides.

Adjourn Meeting

Ms. Gallagher adjourned the meeting at 11:45 a.m. EST.

FPKIMA Open Action Items

Number	Action Statement	POC	Start Date	Target Date	Status
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	12-Jul-11	13-Sep-11	Open
460	The FPKIMA will work with Mozilla to determine what Mozilla will accept if we do not provide CPSs	Wendy Brown	8-May-12	30-Jul-12	Open
464	Ms. Darlene Gore to provide the briefing that was given to the BOAC to Mr. Jeff Jarboe for distribution to the FPKIPA.	Darlene Gore, Jeff Jarboe	10-Jul-12	17-Jul-12	Open
466	Ms. Gallagher to forward complaints about some agencies not accepting external PIV-I and SHA-1 credentials to Ms. Deb Mitchell.	Deb Gallagher	10-Jul-12	17-Jul-12	Open
467	Mr. Slusher will draft language with Mr. Froehlich, Mr. King, and Mr. Silver, to add language about PKI uses and business processes to the FPKI Criticality letter and send the final version to Ms. Gallagher.	Toby Slusher	14-Aug-12	11-Sep-12	Open
468	Ms. Gallagher will submit the final FPKI Criticality Letter to the ICAMSC.	Deb Gallagher	14-Aug-12	30-Sep-12	Open
469	The FPKIMA will send information to the FPKIPA mail list about how to participate in the Mozilla discussion.	Wendy Brown	14-Aug-12	11-Sep-12	Open
470	Mr. Froehlich will lead CPWG discussions to develop a change proposal to add language to the FBCA and Common policies that requires digital signature of supporting documents	Charles Froehlich	14-Aug-12	11-Sep-12	Open
471	The CPWG will review the Common Policy to determine if another change proposal is required to allow for the long-term CRL issued by the Legacy Common Policy CA	Charles Froehlich	14-Aug-12	11-Sep-12	Open
472	Mr. Froehlich will lead discussions in the CPWG to develop a PIV Content Signing change proposal.	Charles Froehlich	14-Aug-12	11-Sep-12	Open

Number	Action Statement	POC	Start Date	Target Date	Status
473	Any Affiliate still cross-certified with the SHA1 FRCA needs to begin providing updates on their plans to transition off the SHA1 FRCA prior to December 31, 2013. This includes: DoD, DEA, Illinois, Symantec, CertiPath, and SAFE.	FPKI Affiliates	14-Aug-12	11-Sep-12	Open
474	Mr. Jason Miller will work to obtain more detailed information on the VA remediation efforts.	Jason Miller	14-Aug-12	11-Sep-12	Closed
475	Ms. Gallagher will resubmit the metrics related to the FPKI Security Profile to the FISMA team	Deb Gallagher	14-Aug-12	11-Sep-12	Open